

FILED

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

2019 JAN 29 A 10:02

In the Matter of the Search of)

(Briefly describe the property to be searched
or identify the person by name and address))42838 Falling Leaf Court, Ashburn, Virginia 20148, which is a)
multi-level single family house with a two-car attached garage)

Case No. 1:19-sw-31

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Eastern District of Virginia

(identify the person or describe the property to be searched and give its location):

See Attachment A.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the
property to be seized):

See Attachment B.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.YOU ARE COMMANDED to execute this warrant on or before January 30, 2019

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been
established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge
The Honorable John F. Anderson

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for days (not to exceed 30).☐ until, the facts justifying, the later specific date of .Date and time issued: 1/16/2019/s/ John F. Anderson

United States Magistrate Judge

City and state: Alexandria, VA

Hon. John F. Anderson, United States Magistrate Judge

Printed name and title

1/29/2019
JFA

3:45 pm

Return

Case No.:
1:19-sw-31Date and time warrant executed:
1/24/19 at 8:00 amCopy of warrant and inventory left with:
Maros Kmec / home owner

Inventory made in the presence of:

Maros Kmec

Inventory of the property taken and name of any person(s) seized:

- Contract documents
- Western Digital harddrive, SN: WX41A685FIUR
- Lexar 64GB thumbdrive
- Seagate 4TB hard drive, SN: NA8FLWWK
- Seagate hard drive, SN: NAS2F63J
- Dell laptop x01, SN: 1J93WB2
- Notebooks

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date:

1/28/19

Austin Price

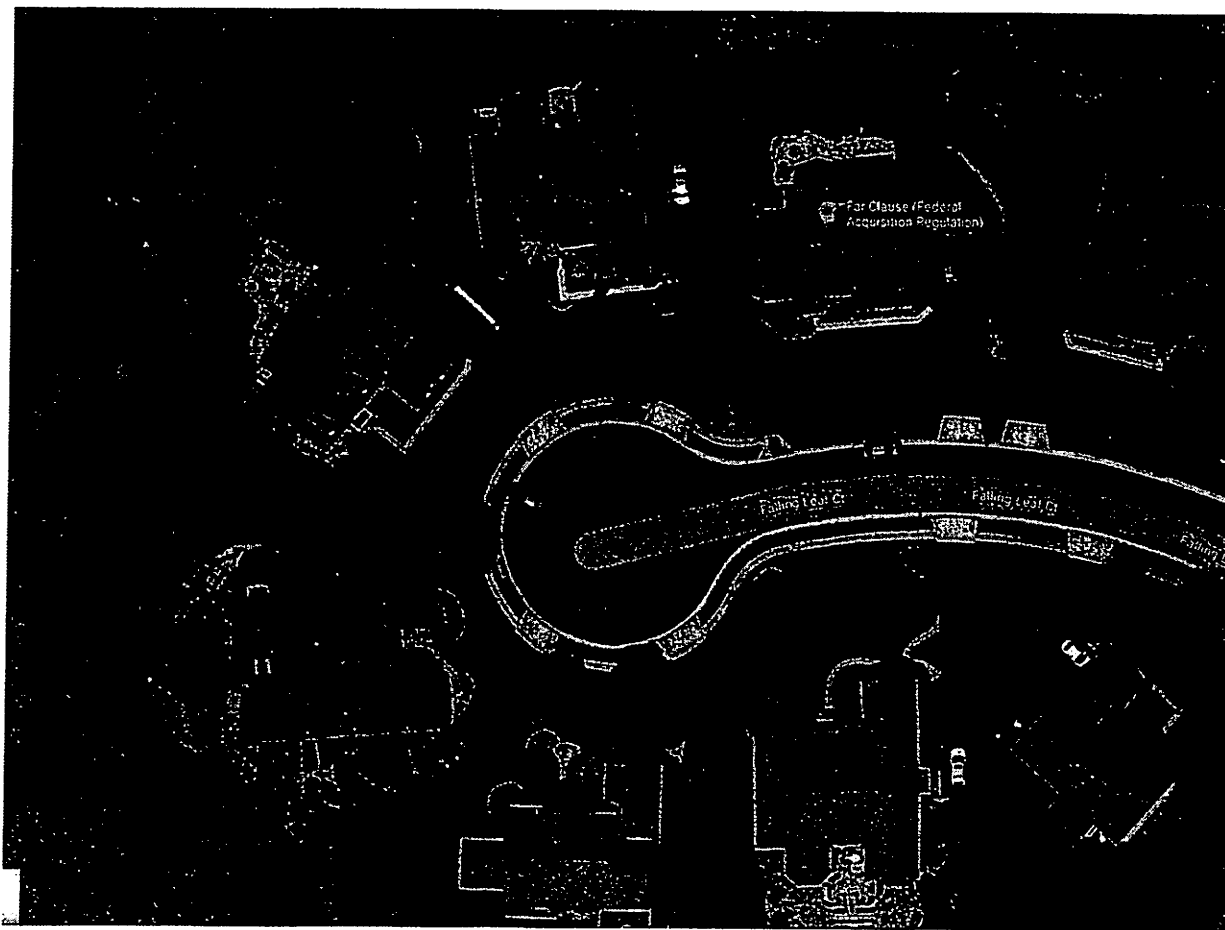
Executing officer's signature

Austin Price, Special Agent

Printed name and title

ATTACHMENT A

The property to be searched is the residence located at 42838 Falling Leaf Court, Ashburn, Virginia 20148. The SUBJECT PREMISES is further depicted in the below photographs and is described as a large single family home on Falling Leaf Court with the numbers "42838" clearly affixed to the home/mailbox and visible from the street. The vehicle has been observed at the SUBJECT PREMISES as recently as January 2, 2019. In addition, the search shall be extended to any locked safe or container within the SUBJECT PREMISES. It shall also be extended to Maros Kmec's Lexus SUV, which he drove to and from work on October 17, 2018.



Google Maps overhead image of 42838 Falling Leaf Court, Ashburn, Virginia 20148

ATTACHMENT B

The following is a list of property to be seized from within the premises known as 42838 Falling Leaf Court, Ashburn, Virginia 20148, a Lexus SUV, and any safes, lockers and closed containers therein, which constitutes evidence, fruits or instrumentalities of violations of the following federal statutes: Title 18, United States Code, Section 1832 (Theft of Trade Secrets); Title 18, United States Code, Section 2314 (Interstate Transportation of Stolen Property); Title 18, United States Code, Section 1343 (Wire Fraud); Title 18, United States Code, Section 2 (Aiding and Abetting the foregoing offenses); and Title 18, United States Code, Section 371 (Conspiracy to commit the foregoing offenses).

- a) Any and all financial, business, scientific, technical, economic and engineering information, of any form or type, relating to ADSI's or another company's proprietary information or trade secrets, which appears to be legally or equitably owned by, or licensed to, ADSI or another company, including, but not limited, to patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs and codes, and contracts, stored in any manner such as physically, electronically, graphically, photographically or in writing.
- b) Any other confidential information related to ADSI's and any other company's proprietary information or trade secrets, including but not limited to business records which reflect the source, development, marketing or sale of proprietary information or trade secret data, including, but not limited to, customer lists, customer files, customer correspondence, customer billing records, pick-up and delivery tickets, employee and drivers records, insurance

records, financial records, invoices, contracts, bank records, investment records, canceled checks, drafts, money orders, cash, memoranda, correspondence, handwritten notes, notebooks, telephone directories, address listings, and calendars.

- c) Any and all records of measures taken to keep secret proprietary information or trade secret data, including but not limited to exit interviews, confidentiality agreements (e.g., with employees, vendors, customers and competitors), non-compete agreements, employee contracts, employee handbooks or manuals, non-disclosure and unauthorized use warnings.
- d) Any and all records of legal or equitable ownership of, or license in, proprietary information or trade secret data by ADSI or any other company, and use or intended use of proprietary or trade secret data.
- e) Any and all records or other materials relating to the theft, misappropriation, unauthorized conversion, receipt, purchase or possession by any person[s] or entit[ies] other than ADSI of the proprietary information or trade secret data including, but not limited to, documents relating to the formation of corporate entities, business plans and venture capital proposals.
- f) Any and all records of employment offers and/or negotiation of employment terms by such person[s] or entit[ies].
- g) Any communications between such person[s] or entit[ies] and parties other than ADSI relating to proprietary information or trade secret data.
- h) Resource or reference materials relating to such financial, business, scientific, technical, economic and engineering information, including, but not limited

to, technical manuals, trade association documents, treatises.

- i) Conversations, whether through text message or other applications, where Maros Kmec discusses ADSI's proprietary information or trade secret data with other individuals.
- j) Computers and associated devices which could be used to transmit or store any of the above described financial, business, scientific, technical, economic and engineering information and books and records, including but not limited to:

- Computer Hardware – all equipment that can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data, including any data-processing devices (such as central processing units, memory typewriters, self-contained "laptop" or "notebook" computers, mobile phones, including "smart" phones, tablets, and server computers), internal and peripheral storage devices (such as fixed disks, external hard disks/drives, including but not limited to, the Seagate external hard drive discussed in the affidavit, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices), peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers), related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling

devices, and electronic tone-generating devices), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks);

- Digital Storage Devices – any and all tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, including external hard drives, monitors, computer printers, modems, tape drives, thumb drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, tape systems and hard drive and other computer related operation equipment, in addition to computer photographs, Graphic Interchange formats and/or photographs, slides or other visual depictions of such Graphic Interchange format equipment which may be, or are used to send, receive, or store documents in an electronic format;
- Computer Software – digital information that can be interpreted by a computer and any of its related components to direct the way it works, stored in electronic, magnetic, optical, or other digital form, including but not limited to programs to run operating systems and applications (like word-processing, graphics, or spreadsheet programs, utilities, compilers, interpreters, and communications programs);
- Computer-related Documentation – written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, software, or other related items; and

- Computer Passwords and Other Data Security Devices – passwords (usually but not always a string of alpha-numeric characters) and other data security devices, including but not limited to encryption devices, chips, and circuit boards, programming code that creates “test” keys or “hot” keys which perform certain pre-set security functions when touched, software or code which encrypts, compresses, hides, or “booby-traps” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

Definitions

As used above, the terms “information,” “records,” “materials” and “documents” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any electrical, electronic, or magnetic form (such as any information on an electronic or magnetic storage device, including floppy diskettes, hard disks and external hard drives, ZIP disks, CD-ROMs, optical discs, backup tapes, printer buffers, smart cards, memory calculators, pagers, personal digital assistants such as Palm Pilot computers, mobile phones, including “smart phones,” and tablets, as well as printouts or readouts from any magnetic storage device); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies).